Infosec Policies and Strategies
GeorgiaTech
6 Nov 2012

The International Cyber-Security Ecosystem

Tony Rutkowski
GaTech Senior Distinguished Fellow
ITU-T Rapporteur for Cybersecurity 2009-2012
tony@yaanatech.com

What is cyber security

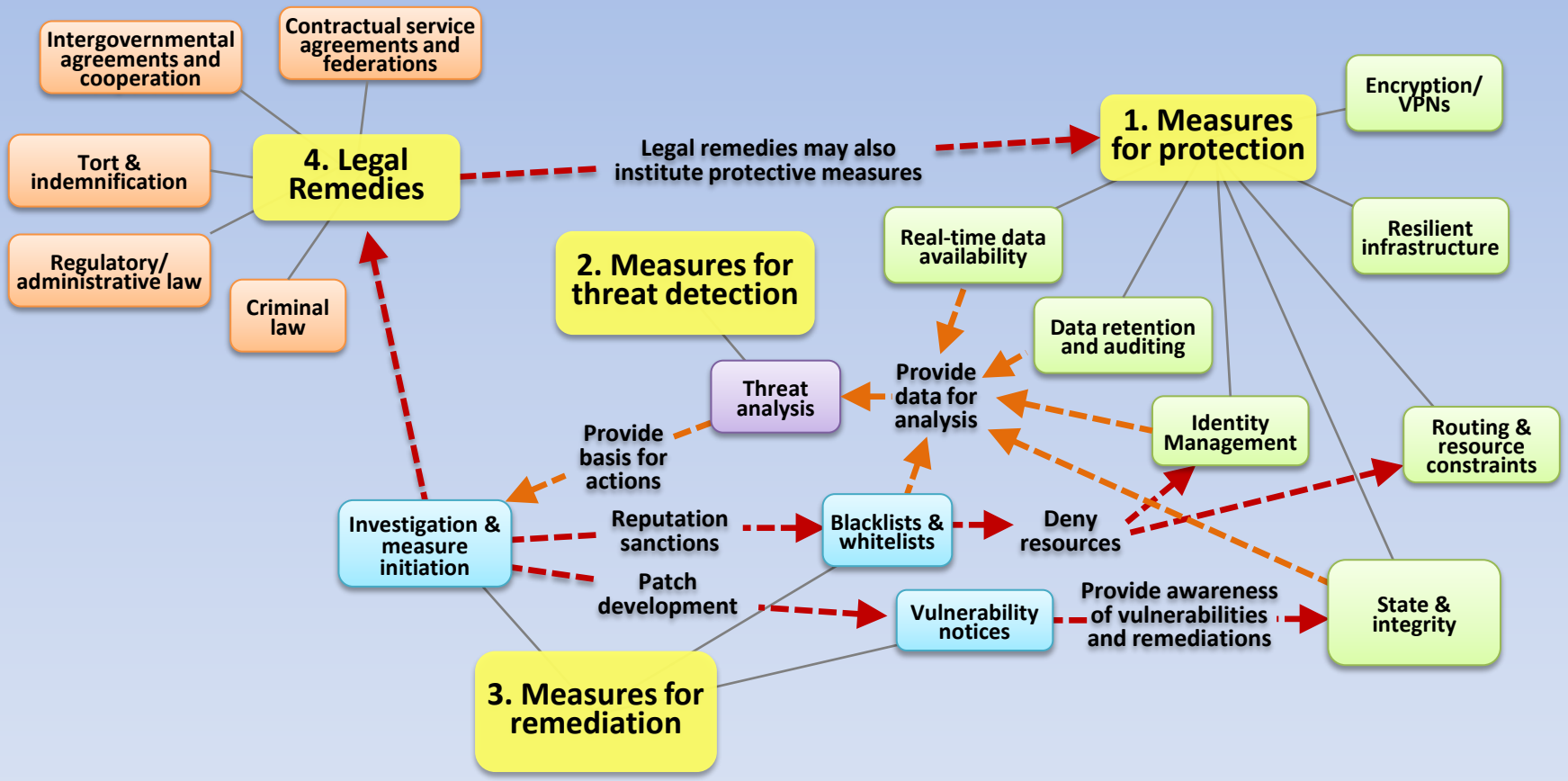
Cyber security is the discovery, analysis and mitigation of vulnerabilities and diminished trust in “virtual” computer-based entities and services occurring because of

- Globalization of supply chains
- Exponentially increasing complexity of devices and computer code
- Increasingly open, global networks and devices
- Accidental and purposeful exploitations and barriers by human and institutional actors

The challenges and caveats

- Trust challenges exist for all computer based devices and networks
  - The threats are never disappearing
    - Giga human actions + giga devices + giga components + giga lines of executable software + constant change
    - One can only manage the risk
  - Principal threats are unknown vulnerabilities and insider human actions
  - The problems exist for all network infrastructures and are not unique to “the Internet”
- The cloud virtualization environment creates new challenges
- Lawful Interception, Data Retention, Content Control and Cyberwar are out of scope
- Some argue that the existing networking computational paradigms are fundamentally flawed and need to be reinvented
  - Ongoing research – Peter Neumann’s “killing the computer” http://www.nytimes.com/2012/10/30/science/rethinking-the-computer-at-80.html

The GaTech cyber security diagram



= information exchange for analysis

= information exchange for actions

Goodman-Lukasik-Rutkowski Model

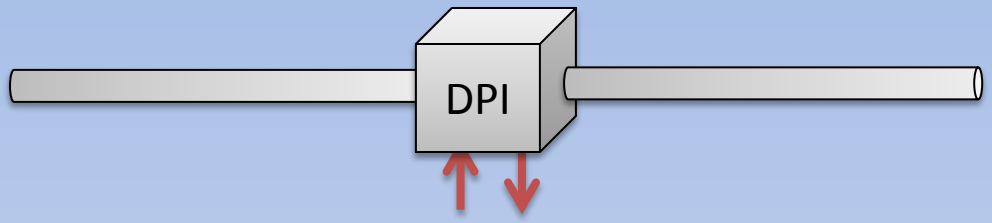
Ecosystem components

- Operations
  - Assumed to be based on trust and legal relationships
  - Focus is on structured, trusted information exchange platforms
- Principal Platforms
  - Technical & operational measures & controls
    - Vulnerability mitigation
    - Threat detection
    - Remediation
    - Certification
  - Legal
- Forums
  - Industry collaboration
    - Standards
  - Legal/regulatory governmental/intergovernmental

Cyber security policy

- What constitutes cyber security
- How to implement and evolve capabilities
  - Sharing information
    - What is required and among whom
    - What trust circles exist
  - Infrastructure and operations mandates
    - Who has what jurisdiction and authority
  - Who pays
  - Who controls
- Forum choices
  - Most legacy organizations are highly ineffectual
  - Global multilateral organizations have zero trust

Fog of cyber security policy



- Necessary to manage traffic, yet can counter “net neutrality”
- Necessary to implement cyber security and cyber war defense, yet can control content
- Necessary for lawful interception, yet can perform unlawful interception

Challenge of cyber security stovepipes

- When a topic becomes important and popular, every forum becomes becomes a venue
- Venues and the people who play in them tend to evangelize their own role and singularity
- Forums ignore the Dirty Harry admonition “a venue’s gotta know its limitations”
- There are no incentives nor effective means for cross organization discovery and collaboration
- There are no good models for intergovernmental activities terminating themselves

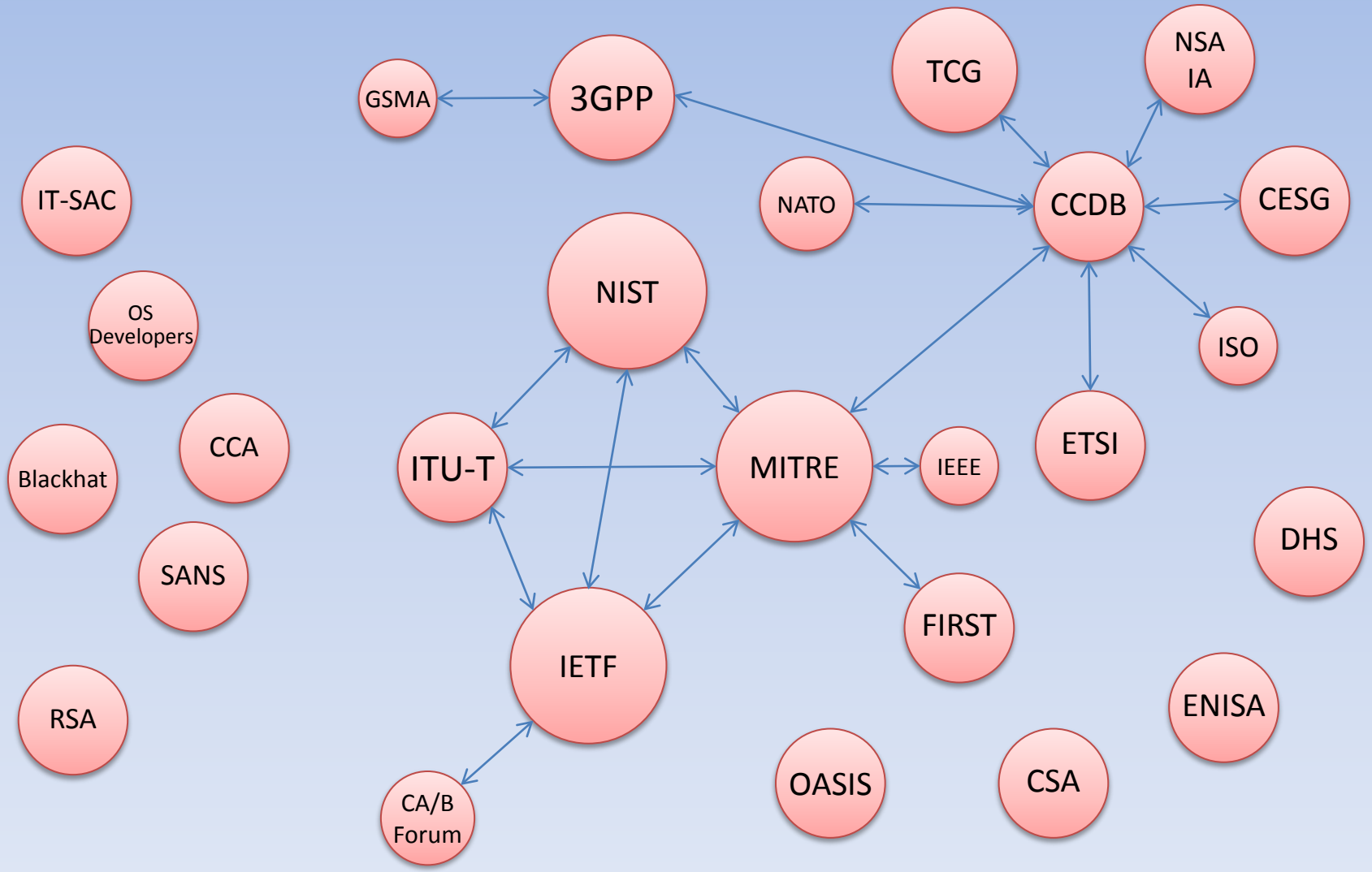
Cyber security “extreme agendas”

- Russia
  - Long history of controlling content and communications
  - Limited skills and political penchants favor global multilateral organizations
  - Significant focus on cyberwar
- Korea
  - Academics with limited skills trolling for money tend to drive bizarre multilateral projects
- MEA
  - Minimal resources and skills
  - General strong government interest in controlling content and communications
- ITU elected officials
  - “Cyber-pander” to expand jurisdiction and bureaucratic empires
  - Serve as nation state agents
- China
  - Principal interest is growing economic opportunities
  - Flush with resources and interested in leadership positions and skill set building
  - Strong government interest in controlling content and communications

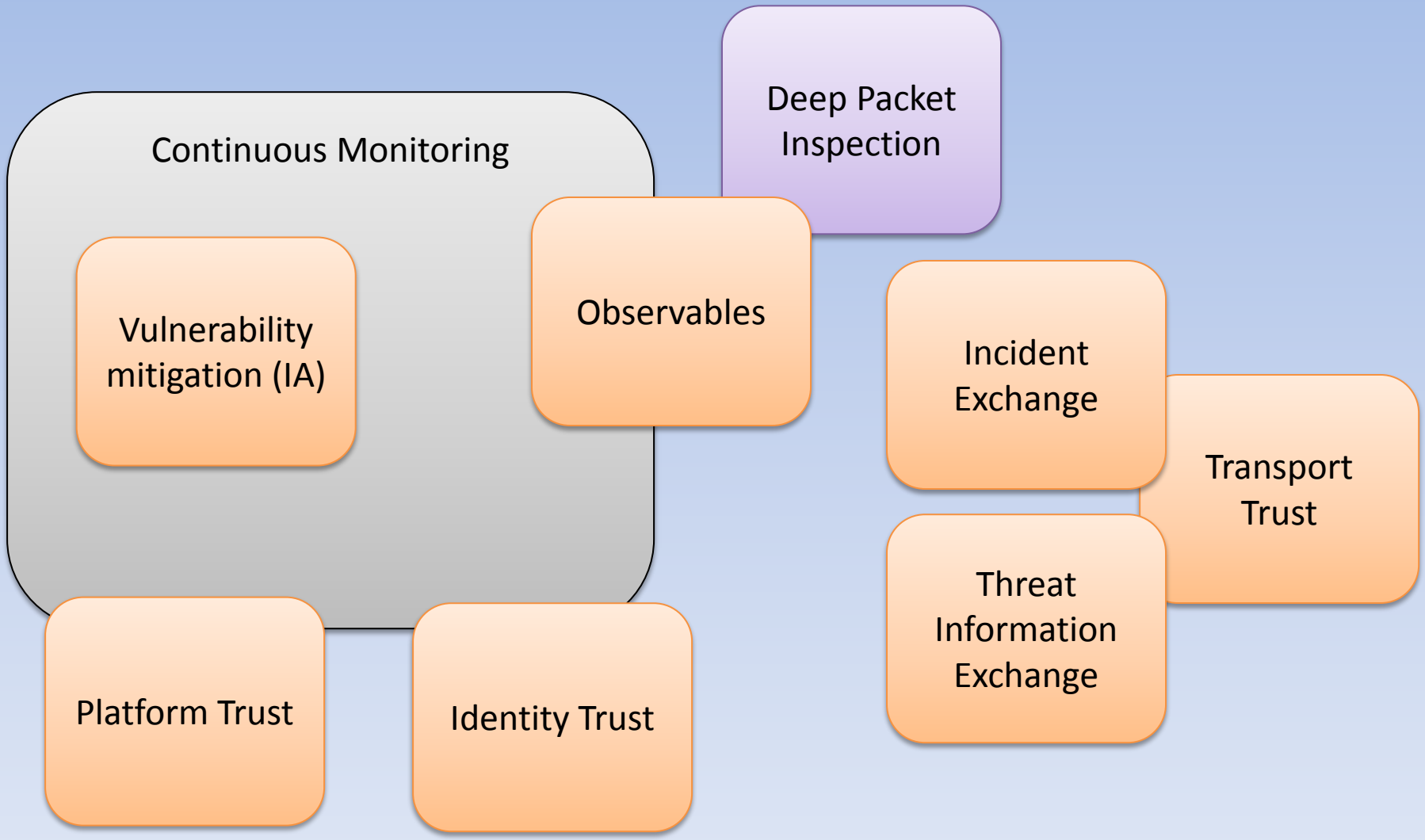
Legal platforms

- Common Criteria Recognition Agreement (CCRA)
- Convention on Cybercrime (CoE)
- NATO agreement
- ITU Constitution (ITU)
- Potential intergovernmental legal platforms
  - International Telecommunication Regulations (ITU)
  - General Agreement on Trade in Services (WTO)
  - Group of 16 Agreement (UN)
  - Trust agreement models (UNCITRAL)

Cyber Security Ecosystem Forums



Important New Cyber Security Ecosystem Platforms



Tony Sager's Top Twenty
Consortium for Cybersecurity Action (CCA)

- **20 Critical Security Controls - Version 4.0**
- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

Deep dive on industry forums 1a

- **MITRE**
  - Many of the basic concepts for information assurance as well as their standardization have occurred within a broad array of development and standardization groups maintained by The MITRE Corporation over the past decade
  - MITRE is a non-profit R&D organization that supports the U.S. network security community in much the same way as Bellcore was once maintained as a common standards development organization for the telecommunications industry
  - MITRE maintains a very extensive array of public-private industry standards activities related to information systems assurance.
- **NIST**
  - The National Institute of Standards and Technology is an agency within the U.S. Department of Commerce that has a responsibility for developing and publishing Information Assurance and other security related standards
  - NIST has been given global SDO status by the ITU-T as an A.5 recognized standards body. Many of the standards developed within the MITRE communities become published by NIST in several forms such as NISTRs, Special Pubs, and FIPS
  - It has also been accorded similar status by many national and regional bodies such as the European Commission
  - Its standards also become mandates for many U.S. government network infrastructures. See The SCAP Community.

Deep dive on industry forums 1b

- **TCG**
  - The Trusted Computing Group is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms
  - Many of TCG's specifications are unique in providing unique trust capabilities at the hardware and low-level operating system level, especially those that facilitate traceability through supply chains
  - 3GPP SA3 (GSM security) has been working closely with TCG, which has a number of relevant IA workgroups: Infrastructure, Mobile Platform, Application Client, Server Specific, Storage, Multi-tenant Infrastructure, Trusted Network Connect, Trusted Platform Module, Software Stack, and Virtualized Platform
- **FIRST**
  - The Forum for Incident Response and Security Teams brings together a variety of computer security incident response teams from government, commercial, and educational organizations
  - FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large
  - Its CVSS SIG is responsible for the Common Vulnerability Scoring System
  - CVSS is a utility used in conjunction with CVE to rate the impact of the vulnerability.

Deep dive on industry forums 1c

- **IETF**
  - The Internet Engineering Task Force more than a decade ago facilitated IA threat analysis through the development of IODEF – an means for structured exchange of incident information
  - The activity surrounding IODEF scaled significantly last year with the creation of a dedicated working group, MILE
  - During the past year, a significant portion of the IA community sought to move stable work from MITRE and NIST venues to a new IETF working group called SACM (Security Automation and Continuous Monitoring)
  - It is expected that this group will be formed at the IETF, November 2012 meeting
- **CCA**
  - The Consortium for Cybersecurity Action (CCA), a newly-formed international consortium of government agencies and private organizations from around the world
  - Serves as an ongoing mechanism to bring together community expertise on attacks and threats; identify and prioritize the most effective defensive controls (based on performance in stopping attacks); identify tools and processes to support implementation; encourage and support adoption of the Critical Controls by organizations, standards bodies, and governments; and enable the world community to share cyber defense information and effective practices
  - CCA's director is Tony Sager
  - The Critical Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to both manage and measure the effectiveness of their defenses
  - The controls are designed to complement existing standards, frameworks, compliance schemes, etc. by bringing priority and focus to the most critical threat and highest payoff defenses, while providing a common baseline for action against the risks that we all face

Deep dive on industry forums 2

- **ITU-T**
  - The International Telecommunication Union Telecommunication Standardization Sector is an intergovernmental standards body that has existed for many years
  - For the past four years, the ITU-T maintained a rapporteur group known as Q4/17 that brought together representatives of nearly all of the organizations in this section as part of a cybersecurity standards initiative to identify key IA platforms
  - It produced an overview standard designated X.1500 and imported a few of the specifications as ITU-T Recommendations
  - The ITU-T plans to maintain the X.1500 appendix as a kind of living document that identifies important IA and other cybersecurity specifications important to industry
  - Existence as an intergovernmental treaty organization under the control of 193 Member nations makes it highly political and diminished use for cyber security purposes
- **CCDB**
  - The Common Criteria Recognition Arrangement is an organization constituted by the principal information systems assurance agencies among 26 nations to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles
  - The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for the CCRA
  - These standards – most of which are initially developed in the above IA communities - are managed and published by the Common Criteria Development Board (CCDB), some of which have been republished by ISO SC27
  - The CCRA has an extensive global certification process
  - A new CCRA vision statement looks to significantly expand the scope, membership, and applicability of the CCRA

Deep dive on industry forums 3

- **3GPP**
  - The 3rd Generation Partnership Project is the principal global standards body for mobile infrastructure and services
  - Among the four Technical Specification Groups (TSG) Service & Systems Aspects (SA) and Core Network & Terminals (CT) focus on security assurance
  - Within SA, Working Group (WG) SA3 has embarked on new work to develop a scheme to provide assurance that network elements are built securely and that security levels can be evaluated
  - A Study Item on *Security Assurance Methodology for 3GPP Network Elements (SECAM)* is currently underway
- **GSMA**
  - The GSM Association represents the interests of mobile operators worldwide
  - Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem. GSMA works closely with 3GPP
  - The GSMA's Security Accreditation Scheme (SAS) enables all GSM operators, regardless of their resources or experience, to assess smart card suppliers' security
  - The GSMA Security Working Group (SG) is charged with maintaining the overall security of the GSM mobile radio system for the operators. It publishes a network risks document and advises on security related matters and maintains a formal reporting method (SWAP) on significant security threats
- **ISO**
  - The International Organization for Standardization is a private standards body consisting of many independent standards committees
  - Its Standards Committee 27 republishes for free some CCDB IA standards as ISO/IEC 15408-1, -2, and -3
- **ETSI**
  - The European Telecommunications Standardization Institute produces globally applicable standards for information and communications technologies. The European Union provides special recognition to some ETSI standards designated European Standards
  - The ETSI TISPAN Technical Committee several years ago published a Security Design Guide on the Method for application of Common Criteria to ETSI deliverables and then built on the work, including a recent standard on Method and proforma for Threat, Risk, Vulnerability Analysis
  - This work continues under two new groups - End-to-End Network Architectures (E2NA) and Technical Committee Network Technologies (NTECH)

Deep dive on industry forums 4

- **CA/B Forum**
  - The Certification Authority Browser Forum (CA/Browser Forum) is standards forum constituted by leading certification authorities (CAs) and vendors of Internet browser software and other applications
  - Worldwide to prepare the specification for the implementation of the Extended Validation (EV) SSL Certificate
  - EV-CERTs are a way of providing a heightened security for network transactions including software identity. Its standard has also been published by ETSI as standard TS102042
- **IEEE**
  - The IEEE Standards Association is a private standards body consisting of many independent standards committees
  - Its IC Security Group Malware Working Group is developing standards for the exchange of malware metadata
  - It works closely with the MITRE Malware Attribute Enumeration and Characterization (MAEC) standards group
  - These platforms are essential to Information System Assurance platforms for thwarting exploits of system vulnerabilities
- **NATO**
  - The NATO Consultation, Command and Control Organization (NC3O) was formed in 1996
  - Its main objective is to provide a coherent, secure and interoperable C3 capability to the NATO
  - Within the organization, the Information Assurance Subcommittee establishes requirements for member infrastructure
  - It collaborates with numerous other IA standards fora and specifies standards that generally leverage those of other bodies described above.

Developer conferences and activities

- There are many conferences that are constantly convened and serve as important components of the IA ecosystem
- There are many IA specific events
- The largest is the annual IT-SAC
- Generic events
  - RSA conferences
  - BlackHat conferences (which now includes a Mobile Device Security Summit)
  - SANS conferences
  - These conferences typically include a broad array of vendors
  - The annual ETSI Security Workshop also brings together some of the IA community.

Protection Platforms 1

- The various methodologies span multiple for a
- Most are adopted by multiple for a
- In many cases, the responsibility for evolving the standard migrates among bodies
- The most extensive and current of these methodology listings, complete with URLs, is maintained on MITRE's "Making Security Measureable" categories site consisting of four groups
  - Languages/Formats
  - Registries
  - Compatible Usage
  - Standardized Processes

Protection Platforms 2

- The rapid evolution of methodologies is exemplified by the recent introduction of a new platform known as the Vulnerability Data Model by NIST
  - NIST/NSA Continuous Security Monitoring
  - the exchange of structured threat information
- Security assurance and hardening are not static, but constantly evolving
- The continuing exchange of current threat information is critical to reducing the risks of network elements and their use
- The GSMA both through its Security Accreditation Scheme as well as its Security Weakness Apparatus/Products Knowledge Base (SWAP) maintains means for accreditation and information exchange

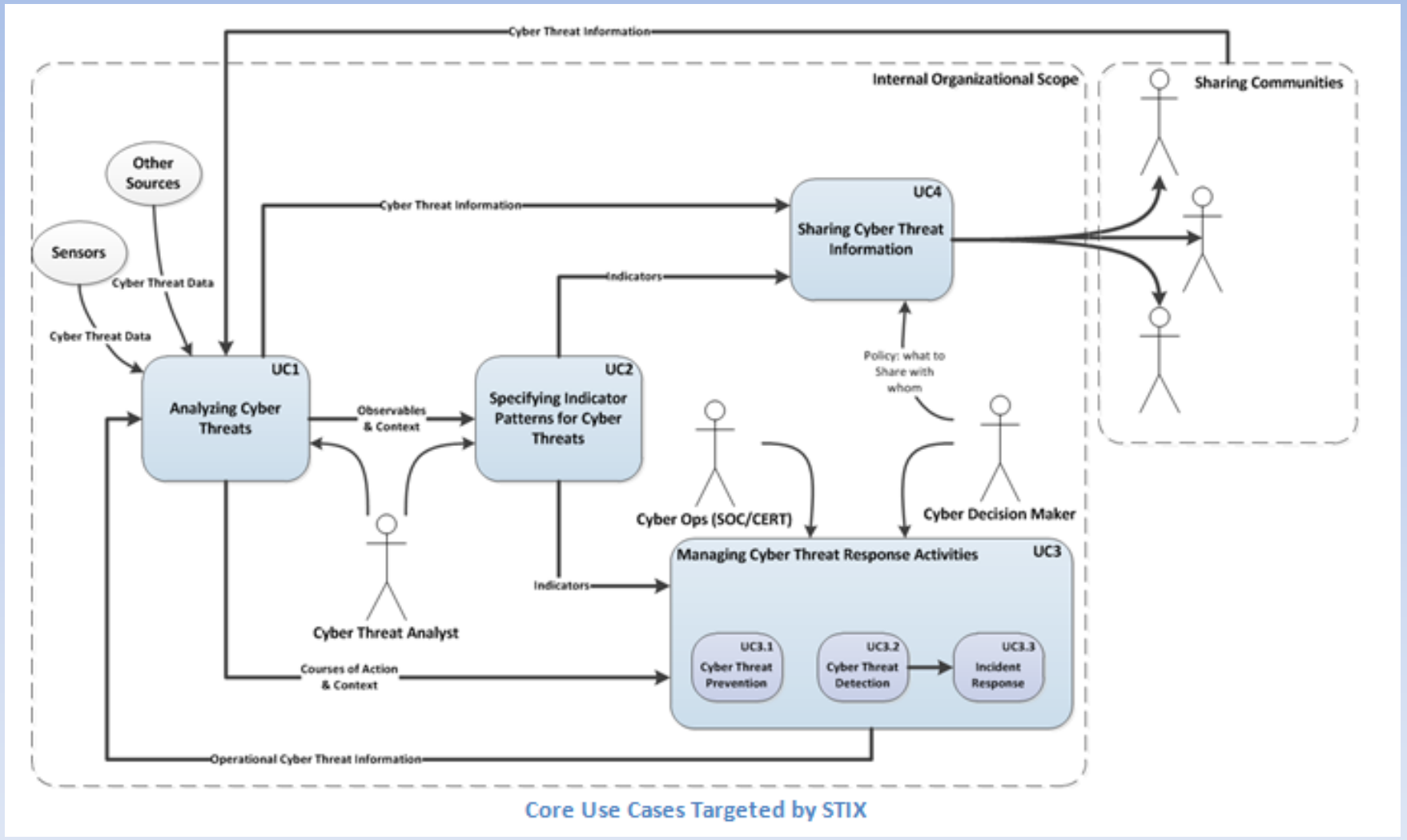
Protection platforms 3

- The CCDB system assurance specification suite was recently revised in Sept 2012, and its standards have the benefit of explicit acceptance of Australia Canada, France, Germany, Japan, Netherlands, New Zealand, Spain, United Kingdom, and the United States. It is also usefully constantly revised to reflect development methodologies described above, as well as re-publication by ISO/IEC
- The ITU-T Cybersecurity Information Exchange (CYBEX) methodology in Rec. ITU-T X.1500 is based entirely on many of these platforms, and provides an independent international confirmation of acceptance together with language translations as well as significant involvement of Japan's IA community

Threat Exchange Platform (STIX)

- The cyber threat intelligence community is facing a challenge in the acquisition, integration, and exchange of real-time attack information
- Threat actors exploit the very complex, dynamic, distributed network and service architectures which exist today
  - Those architectures include vast arrays of mobile devices, apps, and cloud computing and virtualization implementations found in large data centres
- The cyber threat intelligence community is relying on coherent integration of standardized, structured representations of the relevant information including attack pattern analysis
  - Structured Threat Information eXpression (STIX™) is the most advanced example of these approaches
  - STIX is trademarked by USGOV research corporation MITRE but has no constraints on its use
  - STIX's description is found in a recently published white paper <measurablesecurity.mitre.org/docs/STIX-Whitepaper.pdf>

STIX Core Use Cases



Core Use Cases Targeted by STIX

Structured Threat Information eXpression architecture v0.3